WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Hybrid Trace Back Technique for Preventing DDOS Attack on Wireless Senser Networks

Prof. Satish Soni[1], Ashiya Parween[2]

[1]Professor & Head of Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India
[2]Scholar, Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India

ABSTRACT:

Recent advances in wireless communications and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate un-tethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Since large number of sensor nodes is densely deployed, neighbor nodes may be very close to each other. Hence, multi-hop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multi-hop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication.

1. Introduction:

Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following two ways:

- Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.
- Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.
- A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.

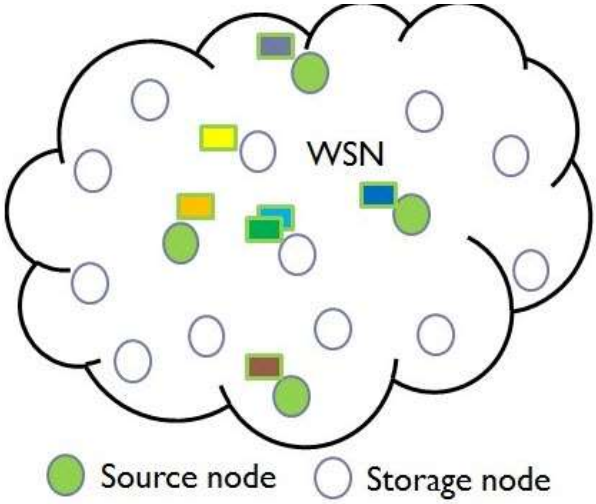

Fig 1.1: An Example visualization of Wireless sensor network

The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data

to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. While this is more convenient for the patient, it also allows the doctor to better understand the patient's current condition. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We envision that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are outlined below:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.

2. Literature Review

Yan, Qiao, F. Richard Yu, Qingxiang Gong2016 [1] Distributed Denial of Service (DDoS) attacks in cloud computing environments are growing due to the essential characteristics of cloud computing. With recent advances in software-defined networking (SDN), SDN-based cloud brings them new chances to defeat DDoS attacks in cloud computing environments. Nevertheless, there is a contradictory relationship between SDN and DDoS attacks. On one hand, the capabilities of SDN, including software-based traffic analysis, centralized control, global view of the network, dynamic updating of forwarding rules, make it easier to detect and react to DDoS attacks. On the other hand, the security of SDN itself remains to be addressed, and potential DDoS vulnerabilities exist across SDN platforms. In this paper, they discuss the new trends and characteristics of DDoS attacks in cloud computing, and provide a comprehensive survey of defense mechanisms against DDoS attacks using SDN. In addition, they review the studies about launching DDoS attacks on SDN, as well as the methods against DDoS attacks in SDN. To the best of Their knowledge, the contradictory relationship between SDN and DDoS attacks has not been well addressed in previous works. This work can help to understand how to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments and how to prevent SDN itself from becoming a victim of DDoS attacks, which are important for the smooth evolution of SDN-based cloud without the distraction of DDoS attacks.

Huang, Qiang, Hisashi Kobayashi2003 [2] As the number of wireless users increases and as more powerful mobile devices become available for lower cost, distributed denial-of-service (DDoS) attacks will pose an increasingly real threat to wireless network security. In this paper, mathematical models are established to analyze different types of DDoS flooding traffic that could be launched in 3G wireless networks. Traffic information obtained from the model can be used to assess whether resources of a given system are vulnerable to certain types of attacks. The feasibility of launching DDoS attacks in wireless ad hoc networks is also discussed.

Latif, Rabia, Haider Abbas, and Saïd Assar2014 [3] Wireless Body Area Networks (WBANs) have emerged as a promising technology that has shown enormous potential in improving the quality of healthcare, and has thus found a broad range of medical applications from ubiquitous health monitoring to emergency medical response systems. The huge amount of highly sensitive data collected and generated by WBAN nodes requires an ascendable and secure storage and processing infrastructure. Given the limited resources of WBAN nodes for storage and processing, the integration of WBANs and cloud computing may provide a powerful solution. However, despite the benefits of cloud-assisted WBAN, several security issues and challenges remain. Among these, data availability is the most nagging security issue. The most serious threat to data availability is a distributed denial of service (DDoS) attack that directly affects the all-time availability of a patient's data. The existing solutions for standalone WBANs and sensor networks are not applicable in the cloud. The purpose of this review paper is to identify the most threatening types of DDoS attacks affecting the availability of a cloud-assisted WBAN and review the state-of-the-art detection mechanisms for the identified DDoS attacks.

3: METHODOLOGY

3.1 Denial of Service in Sensor Networks

Sensor networks hold the promise of facilitating large-scale, real-time data processing in complex environments. Their foreseeable applications will help protect and monitor military, environmental, safety-critical, or domestic infrastructures and resources. In these and other vital or security-sensitive deployments, keeping the network available for its intended use is essential. The stakes are high: Denial-of-service (DoS) attacks against such networks may permit real-world damage to the health and safety of people. Without proper security mechanisms, networks will be confined to limited, controlled

environments, negating much of the promise they hold. The limited ability of individual sensor nodes to thwart failure or attack makes ensuring network availability more difficult.

To identify DoS vulnerabilities, we analyze two effective sensor network protocols that did not initially consider security. These examples demonstrate that consideration of security at design time is the best way to ensure successful network deployment.

3.2 Theory And Application

Advances in miniaturization combined with an insatiable appetite for previously unrealizable information gathering have led to the development of new kinds of networks. In many areas, static infrastructures are giving way to dynamic ad hoc networks.

One manifestation of these trends is the development of highly application-dependent sensor networks. Developers build sensor networks to collect and analyze low-level data from an environment of interest. Accomplishing the network's goal often depends on local cooperation, aggregation, or data processing because individual nodes have limited capabilities. Physically small, nodes have tiny or irreplaceable power reserves, communicate wirelessly, and may not possess unique identifiers. Further, they

must form ad hoc relationships in a dense network with little or no preexisting infrastructure. Protocols and algorithms operating in the network must support large-scale distribution, often with only localized interactions among nodes. The network must continue operating even after significant node failure, and it must meet real-time requirements. In addition to the limitations imposed by applicationdependent deadlines, because it reflects a changing environment, the data the network gathers may intrinsically be valid for only a short time.

Sensor networks may be deployed in a host of different environments, and they often figure into military scenarios. These networks may gather intelligence in battlefield conditions, track enemy troop movements, monitor a secured zone for activity, or measure damage and casualties. An airplane or artillery could deploy these networks to otherwise unreachable regions.

Although military applications may be the easiest to imagine, much broader opportunities await. Sensor networks could form an impromptu communications network for rescue personnel at disaster sites, or they could themselves help locate casualties. They could monitor conditions at the rim of a volcano, along an earthquake fault, or around a critical water reservoir. Such networks could also provide always-on monitoring of home healthcare for the elderly or detect a chemical or biological threat in an airport or stadium.

Because of their low cost and low overhead, sensor networks can be deployed for civic-event monitoring, then discarded. Longer-lived networks could be periodically refreshed by new deployments, which must integrate themselves into the existing sensor network. The network must be resilient to individual node failure, since at any time nodes could be destroyed, exhaust their power, or fail due to imperfections in large-scale manufacturing processes.

For many sensor network applications, security is critical. Some face not only a harsh environment but also active and intelligent opposition, which makes the need for battlefield resistance to location, destruction, and subversion obvious. Less obvious, but just as important, are the demands in other arenas.

- **Disasters**. It may be necessary to protect the location and status of casualties from unauthorized disclosure—particularly if the disaster relates to ongoing terrorist activities instead of natural causes.
- **Public safety**. False alarms about chemical, biological, or environmental threats could cause panic or disregard for warning systems. An attack on the system's availability could precede a real attack on the protected resource.
- **Home healthcare**. Because protecting privacy is paramount, only authorized users can query or monitor the network. These networks also can form critical pieces of an accident-notification chain, thus they must be protected from failure.

Protocols and software applications should consider security in their original designs as must sensor networks, especially regarding resisting attacks on network availability. Attempts to add security afterwards usually prove unsuccessful.

3.3 The Denial of Services Threate

Strictly speaking, although we usually use the term to refer to an adversary's attempt to disrupt, subvert, or destroy a network, a DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS. Although attackers commonly use the Internet to exploit software bugs when making DoS attacks, here we consider primarily protocol- or design-level vulnerabilities.

Determining if a fault or collection of faults is the result of an intentional DoS attack presents a concern of its own—one that becomes even more difficult in large-scale deployments, which may have a higher nominal failure rate of individual nodes.

An intrusion-detection system monitors a host or network for suspicious activity patterns such as those that match some preprogrammed or possibly learned rules about what constitutes normal or abnormal behavior. Although we do not deal with IDS strategies here, some of the research problems overlap, particularly in the area of attack response.

Sensor networks destined for harsh environments should already be designed to continue functioning in the presence of faults. This robustness against physical challenges may prevent some classes of DoS attacks. Fault tolerance may mitigate even node subversion, and efficient protocols will limit opportunities for malicious waste of resources.

Developers must, however, factor the complication of an intelligent, determined adversary into the design separately. For example, they can design sensors to withstand the effects of normal thermal cycles in a desert environment or to cope with transient irregularities in radio propagation. However, this will not be sufficient to thwart an attacker with physical access to the node, who can move or heat and cool the device at will.

4: Result and its Analysis

Table 4.1 and Figure 4.1 show the effect of proposed prevention technique on Throughput with different number of attackers. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent.

Table 4.2 and Figure 4.2 show the effect of proposed prevention technique on Number of Collisions with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions decreases as compared to the collisions of existing prevention scheme.

Attackers	Throughput
1	1714653
2	1617242
3	1530967

Table 4.1: Effect of Proposed Prevention Technique on Throughput with varying number of attackers.

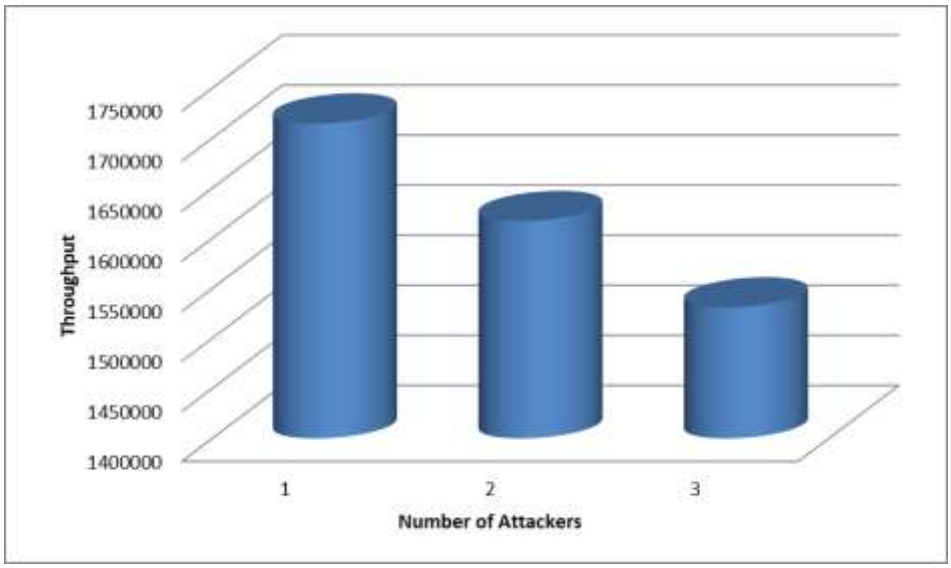

Figure 4.1: Effect of Proposed Prevention Technique on Throughput with varying number of attackers.

Attackers	Existing	Proposed
1	3955	2655
2	4018	2595
3	4175	2676
4	4210	1818
5	4315	2084

Table 4.2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

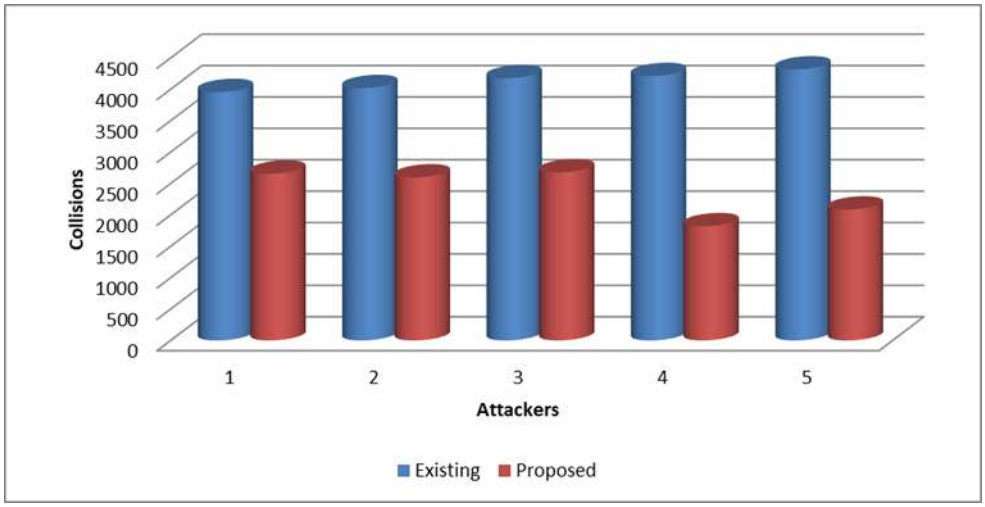

Figure 4.2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

5. CONCLUSION

Handling DDoS attacks in WSNs is quickly becoming more and more complex, and has reached the point where it is difficult to see zombies spread throughout network. On one hand, this hinders an understanding of the DDoS phenomenon. The variety of known attacks creates the impression that the problem space is vast, and hard to explore and address. For classifying attacks and defenses researchers needs a better understanding of the problem and the current solution space. The attack classification criteria in WSNS is even more difficult. After analyzing existing frameworks, we have found three types of DDOS frameworks: victim-end defense frameworks, source-end defense frameworks, and distributed defense frameworks. It is too late for victim-end defense frameworks to respond to DDOS attacks. A source-end defense framework cannot achieve good performance due to lack of attack information. In contrast, a distributed framework can achieve better performance by cooperating among distributed multiple defense subsystems. We propose traceback methodologies to control unwanted traffic by mitigating flooding based DDOS attacks. The work concentrates mainly on the detection algorithm should detect a DDOS attack at the originating source with high reliability. Two main necessities for competent traceback are to swiftly and precisely find possible attackers and other is to filter attack packets so that a host can resume the normal ability to legitimate clients. Most of the continuing IP traceback methods focus on pursuing the locale of attacker's after the attack. This work, we implemented an efficient methodology for discovering possible attackers who retain the DDOS-based attack.

This work ran simulations to illuminate that the methodology that can find the attackers in a short amount of time. DDoS defense systems can be deployed in the network to detect DDoS attacks independently for example, an IDS but these techniques usually fail to trace back the actual attacker. Time to live field. Time to live (TTL) or hop limit is a mechanism that limits the lifespan or lifetime of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded. In computer networking, TTL prevents a data packet from circulating indefinitely. The objective of this research was to control unwanted traffic by mitigating flooding based DDOS attacks using IP Traceback. The IP Traceback algorithm was able to detect a DDOS attack at the originating source with high reliability. The defense framework was effective in distributed network scenario. The DDoS response technique tries to filter most of the attack packets without degrading the Quality of service for genuine user/ traffic.

REFERENCES

[1] Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." *IEEE communications surveys & tutorials* 15, no. 4 (2013): 2046-2069.

[2] Pelechrinis, Konstantinos, Marios Iliofotou, and Srikanth V. Krishnamurthy. "Denial of service attacks in wireless networks: The case of jammers." *IEEE Communications Surveys & Tutorials* 13, no. 2 (2011): 245-257.

[3] Yan, Qiao, F. Richard Yu, Qingxiang Gong, and Jianqiang Li. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." *IEEE Communications Surveys & Tutorials* 18, no. 1 (2016): 602-622.

[4] Huang, Qiang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, and Jinyun Zhang. "Fast authenticated key establishment protocols for self-organizing sensor networks." In *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pp. 141-150. ACM, 2003.

[5] Latif, Rabia, Haider Abbas, and Saïd Assar. "Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review." *Journal of medical systems* 38, no. 11 (2014): 128.

[6] Lupu, Teodor-Grigore, I. Rudas, M. Demiralp, and N. Mastorakis. "Main types of attacks in wireless sensor networks." In *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering*, no. 9. WSEAS, 2009.

[7] Gill, Khusvinder, and Shuang-Hua Yang. "A scheme for preventing denial of service attacks on wireless sensor networks." In *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*, pp. 2603-2609. IEEE, 2009.

[8] Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[9] Yu, Yanli, Keqiu Li, Wanlei Zhou, and Ping Li. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." *Journal of Network and computer Applications* 35, no. 3 (2012): 867-880.

[10] Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." In *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*, pp. 308-311. IEEE, 2011.

[11] Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[12] Arunmozhi, S. A., and Y. Venkataramani. "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks." *arXiv preprint arXiv:1106.1287* (2011).

[13] Nanda, Rohan, and P. Venkata Krishna. "Mitigating denial of service attacks in hierarchical wireless sensor networks." *Network security* 2011, no. 10 (2011): 14-18.

[14] Jan, Mian, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." *Concurrency and Computation: Practice and Experience* (2016).

[15] ELBeltagy, Maha, Sarah Mustafa, Jariya Umka, Laura Lyons, Ahmed Salman, Chur-Yoe Gloria Tu, Nikita Bhalla, Geoffrey Bennett, and Peter M. Wigmore. "Fluoxetine improves the memory deficits caused by the chemotherapy agent 5-fluorouracil." *Behavioural brain research* 208, no. 1 (2010): 112-117.